IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

MR. CHATRIE'S POST-HEARING BRIEF ON "GEOFENCE" GENERAL WARRANT

At the government's direction, Google searched the Location History ("LH") data of "numerous tens of millions" of people in an effort to generate suspects in the robbery. *See* Def. Ex. 21 at 4. It was a dragnet of epic proportions. The warrant seeks to dress up this search in a "three-step" process crafted by Google and the FBI, but that process is no more than a legal fig leaf obscuring the magnitude of the privacy invasion at work. This epic dragnet gave free reign to Google and the government to single out which accounts to search further in steps two and three. It was so overbroad and lacking in particularity that it was the digital equivalent of a general warrant and therefore impermissible under the Fourth Amendment. Mr. Chatrie seeks to suppress all evidence obtained as a result of the geofence warrant, and all fruits thereof.

BACKGROUND

In March 2021, this Court held an evidentiary hearing on Mr. Chatrie's motion to suppress the geofence warrant. *See* ECF 29. Mr. Chatrie had filed that suppression motion in October 2019, based on the sparse facts available to him at that time. What little defense counsel knew about geofence warrants came primarily from newspaper articles and online reports. *See id.* at 4-5. Over the past 18 months, however, investigation revealed significant new facts that have both merited corrections and strengthened Mr. Chatrie's legal arguments.

Specifically, Google filed an *amicus* brief (Def. Ex. 2), unsolicited, as well as four written declarations (Def. Ex. 21; ECF No. 96-2; ECF No. 110-1; Def. Ex. 23) in response to two defense subpoenas *duces tecum* (ECF No. 82; ECF No. 123). In addition, two Google representatives, Marlo McGriff and Sarah Rodriguez, testified in person over the course of two days. Tr. 190–275 282–424, 445–499.[1] The Commonwealth of Virginia provided some information about the qualifications of the magistrate judge who issued the warrant. *See* ECF No. 156. And defense counsel benefited from the expertise of Spencer McInvaille, who forensically examined Mr. Chatrie's phone, prepared two written reports (Def. Ex. 6; Def. Ex. 7), and testified twice in-person. *See* Tr. 16–170; 1/21/20 Tr. 17—139. Furthermore, counsel for Mr. Chatrie cross-examined the Virginia state investigator responsible for obtaining and executing the geofence warrant, Det. Joshua Hylton, Tr. 623–46, and FBI Special Agent Jeremy D'Errico, who offered expert testimony for the government. Tr. 550–93. Finally, three federal magistrates, all in the Northern District of Illinois, have issued opinions, *sua sponte*, regarding geofence warrants. *In re Search Warrant Application for Geofence Location Data Stored at Google* ("Harjani Opinion"), No. 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020); *In re Information Stored at Premises Controlled by Google* ("Fuentes Opinion"), 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google* ("Weisman Opinion"), No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020). Two of the three found the warrants invalid. *See* Fuentes Opinion, 481 F. Supp. 3d at 757; Weisman Opinion, 2020 WL 5491763 at *8. All three of them, however, did so without the benefit of adversarial briefing or the full factual record now before this Court.

Mr. Chatrie submitted a supplemental brief to the Court in May 2020. *See* ECF No. 104. Most significantly, by then, Google clarified that the geofence warrant required searching

[1] All cites to "Tr." refer to the March 4–5, 2021, hearing unless otherwise noted.

"numerous tens of millions" of people, not just the 19 who happened to be near to the bank. *See* Def. Ex. 21 at 4. Google subsequently confirmed this fact at the March hearing and provided additional context that supports Mr. Chatrie's argument in favor of suppression. Mr. Chatrie's arguments have evolved accordingly, and defense counsel has sought to keep the Court abreast of these developments. *See, e.g.,* ECF No. 104 at 2, 4; ECF No. 82 at 2–3. But in the interest of clarity, Mr. Chatrie summarizes the relevant facts as they are currently known.

FACTS

Someone robbed the Call Federal Credit Union in Richmond, Virginia, on May 20, 2019. *See* Def. Ex. 1 at 11. The Chesterfield County Police Department had no suspects. There were plenty of witnesses and surveillance videos, Tr. 607–08, but instead of pursuing traditional investigative techniques, the government turned to Google. Det. Joshua Hylton drafted an application for a "geofence" warrant, a novel digital search that required Google to identify all electronic devices in the area at the time of the robbery, and then provide even more data on devices of interest at the government's discretion. *See* Def. Ex. 1.

Det. Hylton had never received training on geofence warrants. Tr. 627–28. There was no training because there were no law enforcement procedures to follow. Tr. 552-53. In fact, neither the Chesterfield Police nor the FBI, who quickly became involved in this case, trained their investigators on seeking geofence warrants. *Id.*; Tr. 552. Agent D'Errico assisted in the investigation and testified as the government's expert on geofence warrants. Tr. 506–50. Yet, like Det. Hylton, Agent D'Errico admitted he has never received specific training on geofence warrants, from the FBI or from Google. Tr. 551.

This lack of training and absence of procedures does not mean that police conjured the geofence warrant here. The basic contours of a geofence warrant were the unofficial product of

repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018.[2] Tr. 456-57. Google required a warrant because it considers Location History data to be "content" under the Stored Communications Act, 18 U.S.C. § 2703, which requires a warrant to access it. *See* Def. Ex. 2 at 16.[3]

Eventually, Agent D'Errico obtained a "go by" from CCIPS, which "assists" investigators "in the language needed to obtain a geofence search warrant" from Google. Tr. 552; *id.* at 553 ("[W]e follow the steps that [CCIPS and Google] have laid out in order to … make sure that Google understands what we are requesting and that we understand what we'll receive back"). Agent D'Errico does not recall providing this "go by" to Det. Hylton, at least in this case. Tr. 553. But somehow or another—he does not recall—Det. Hylton got one too. Tr. 635. In fact, Det. Hylton had sought a state geofence warrant once before using a local "go by" from another officer, so he used the same template, plugged in the new date and location, and did it again. Tr. 631.

I. Location History

The warrant outlined a three-step process for Google to search users' location data and provide information about nearby devices around the time of the robbery. The warrant did not instruct Google to exclude any types of location data from the search. Rather, it called for searching "each type of Google account," regardless of the device configuration. Def. Ex. 1 at 4, 9. Instead, Google searched one of its three databases: the so-called "Sensorvault" database, which is the repository for "Location History" data. *See* Tr. 211-12; ECF No. 104 at 6-7.

[2] Tr. 456-57 ("CCIPS is an agency that … our counsel engages with to discuss sort of certain procedures that may be relevant for the way that … Google will need to handle these types of requests, especially with reverse Location History being a relatively new type of request"); 476 (repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *see also* Tr. 552-53 (discussing the relationship with CCIPS).

[3] The government disputes Google's characterization of Location History data as user "content," *see* ECF No. 109 at 9; ECF No. 71 at 8, but it has yet to cite to a single case where a subpoena or court order have been sufficient to obtain Location History data.

Location History is a Google feature that logs device location data and creates a timeline on a map of where a user has been with that device. Def. Ex. 21 at 2; Tr. 355. Google likens Location History data to a virtual "journal" of where users have been (with their devices). Def. Ex. 2 at 6; Tr. 204. When Google saves this data, it associates it with unique user accounts it keeps in the "Sensorvault." Def. Ex. 21 at 3; Tr. 130, 314. If a user has the Google Location History enabled, then Google estimates the user's device location using Global Positioning System ("GPS") data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, cell phone location information ("CSLI") from nearby cellular towers, and Internet Protocol ("IP") address information. Tr. 18–19; Def. Ex. 21 at 4, 8–9. Location History is not an "app"; it is a setting on the Google account associated with a device. Once enabled, it records that device's location as often as every two minutes, at all times regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. Tr. 20, 114-15, 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Def. Ex. 21 at 4; Tr. 205. Google has been unable or unwilling to say exactly how many users this was in 2019, but Google acknowledges that it was at least "numerous tens of millions" of people. *Id*.

II. Location History Accuracy

The accuracy of Location History information varies depending on which sources of location data are available to the device at a given time. For example, location data based on GPS signals is usually more accurate than location derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. Google, however, has a preference. Google relies on Wi-Fi signals first, followed by GPS, then Bluetooth, and finally CSLI. Even though GPS data is generally more accurate than Wi-Fi, GPS consumes more resources on the device, diminishing battery life and making it impractical to use frequently. Tr. 519. As a result, Location History data often comes from Wi-Fi data, and that is what happened

in this case. Here, 88% of the coordinates at issue were derived from Wi-Fi signals; the remainder came from GPS. *See* 1/21/20 Tr. at 64. None were derived from Bluetooth, CSLI, or IP address information. *Id.*; *see also* Tr. 173.

Location History data is Google's ***estimation*** of where a device is. Tr. 212. It is not hard data, but is instead Google's best guess at device location based on available information. *See* Def. Ex. 2 at 10–11 n.7 ("In that respect, LH differs from CSLI, which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points …"). As Google puts it, Location History is a "probabilistic estimate," and each data point has its own "margin of error." *Id.* Google uses an unknown algorithm to make this estimation, which Google did not disclose when subpoenaed. *See* ECF No. 82 at 10; ECF No. 85 at 2. Indeed, Location History is different from other types of location data that courts have previously considered and emerges from Google's black box with a fluctuating margin of errors. *See* Tr. 178, 590–91.

When Google reports a set of estimated latitude/longitude coordinates, it also reports a "confidence interval," or "Map Display Radius," to indicate Google's confidence in its estimation. Tr. 38, 212, 530–31. On a map, Google visualizes the coordinates as a "blue dot" and the Display Radius as a "shaded circle" around the dot. *See* Tr. 213; Def. Ex. 21 at 9. The government illustrates this concept (in red) in a report Agent D'Errico prepared, as shown in Figure 1. *See* Gov't Ex. 1 at 18.

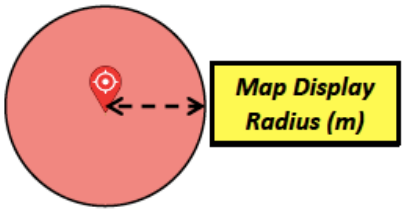
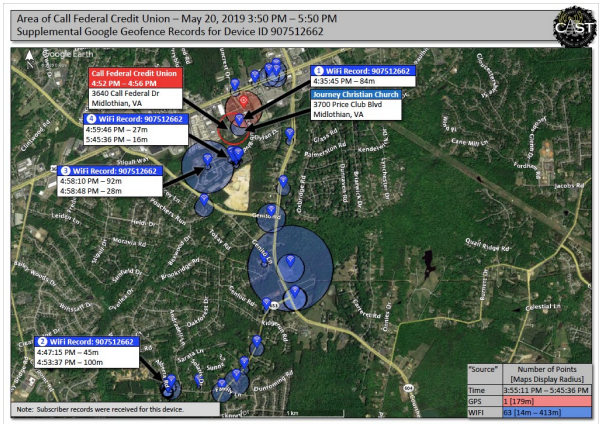


Figure 1

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, *i.e.*, the shaded circle. *See* Tr. 214. The estimated coordinates, recorded as

latitude/longitude, are simply the center point of that circle. *See* Tr. 531 ("If I could, I would draw maps without a center point in it and just a bubble because that's a better representation."). It is equally likely that the device is at the center point as anywhere else in the shaded circle, even off toward the edge. *See* Google, *Find and Improve your Location's Accuracy* (last visited Apr. 26, 2021) ("The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle.").[4] Indeed, Google users may be familiar with this phenomenon, as "in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *Harjani Opinion*, 2020 WL 6343084 at *9.

The Map Display Radius expands and contracts in accordance with Google's confidence in its location estimation. As a result, the accuracy of Location History data varies over time, as illustrated by the varying size of the shaded circles in the government's rendition of user data in this case, as shown in Figure 2 below. ***Figure 2***



Google always aims to be 68% confident that a device is somewhere within the Display Radius. Tr. 39; *see also* Tr. 581 ("68% is approximately the industry standard"). In other words,

[4] *Available at* https://support.google.com/maps/answer/2839911?co=GENIE.Platform%3DAndroid&hl=en.

Google simply changes the size of the Display Radius, or shaded circle, in order to achieve 68% confidence. As Google explains, "The smaller the circle, the more certain the app is about your location." Google, *Find and Improve your Location's Accuracy* at 1. By contrast, a large circle means that Google is less confident in a user's location, indicating that they could be anywhere within a much larger area, the product of a larger Display Radius. *See* Tr. 213, 530-31. There is always a 32% chance a device is outside of the Display Radius altogether. *See* Tr. 213. Or in other words, the odds are better than 1-in-4 that the user's actual location lies beyond the shaded circle.

III. Location History Advertising

Google appears well satisfied with the 68% accuracy industry standard. *See* Tr. 581. According to Google, "the resulting picture of the user's location and movements is sufficiently precise and reliable for the purposes for which it was designed." Def. Ex. 2 at 10 n.7. For Google, Location History has two purposes: (1) to support a "Timeline" map for users, *see* Tr. 195, and (2) to provide targeted advertising based on a user's location, *see* Tr. 22-23, 196–98, 301. Neither function, however, relies on a high degree of accuracy for any data point. Rather, Google infers a user's Timeline from a series of data points even when an "outlier" strays from the logical path. *See* Tr. 195–96. For advertising purposes, Google actively obscures individual device information, preventing businesses from being able to track particular users. *See* Tr. 197.

Google uses Location History for a specific advertising purpose—to calculate "store visit conversions." A "store visit conversion" refers to a user who saw a Google-placed advertisement and then visited the relevant business in person. Tr. 196–97. Location History is not used for other types of location-based advertising, such as "radius targeting," Tr. 197–98, which allows businesses to show an ad to all devices in a given area. As Google explains, "Location History does not power all ads. … [A]ny geotargeting or other use of Location for ads is coming from the

location services at the device level." Tr. 367–68. So, although businesses can use Google to target advertising based on a device's location, they cannot do sousing Location History. Tr. 198.

Regardless of the advertising type, however, Google "never share[s] anyone's location history with a third party." *See* Tr. 197. Google is "not giving user location data over to stores about who was around." Tr. 197. Even when Google uses location data sources other than Location History, such as "Web & App Activity," the smallest possible radius available to advertisers is a kilometer. Tr. 198. This is done for privacy purposes, so that those advertisers do not actually get to see which devices were in the area. Tr. 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. Tr. 199. Advertisers simply cannot get any identifiable information about individual Google users. Tr. 199; *see also* Tr. 23 (explaining that the data in warrant returns is "much different" than what is accessible to advertisers).

IV. Enabling Location History

Google asserts that Location History is an "opt-in" feature for Google users, Def. Ex. 1 at 12, which means that a user must actively enable it at some point in order for it to work. There are, however, many different ways for a user to enable Location History, either through the device settings or through certain Google applications. Def. Ex. 6 at 4; Tr. 74; *see* Tr. 285–86.

One possibility is to enable Location History during the initial setup of a new device. As demonstrated by defense expert Spencer McInvaille during the January 2020 discovery hearing, Google first prompts users to enable Location History during the initial phone setup process. *See* 1/21/20 Tr. at 51. If a user does not opt-in at that point, Google will prompt them to enable Location History through pop-up screens, known as a "consent flow," when opening certain Google applications or using certain Google features.

Another way to enable Location History is to set up Google applications that rely on location information. These apps include the primary Google App (for search queries), as well as Google Maps, Google Photos, and Google Assistant. *See* Tr. 221, 285–86. If a user does not enable Location History while setting up the device, Google prompts them to do so before they can use any of these applications. *See* Tr. 350–52. For example, as the defense demonstrated through video evidence and detailed expert testimony, Google prompts users to enable Location History when first opening Google Maps following the setup of a new phone. 1/21/20 Tr. at 55–56. The whole process took under five minutes and did not mention Location History by name. *Id.* at 56–57.

In this case, a combination of Google data and an extensive forensic analysis of Mr. Chatrie's phone revealed that Location History was likely enabled through the Google Assistant setup process, shortly after midnight on July 9, 2018. Def. Ex. 6 at 4–5; Tr. 76–77, 286–87. Two basic facts led to this conclusion. *See* Def. Ex. 6 at 4–5. First, Google reported that Location History was enabled on Mr. Chatrie's account on July 9, 2018, at approximately 4:09 Universal Time Code ("UTC"), or 12:09 a.m. Eastern time. *See* Def. Ex. 6 at 2; Def. Ex. 23 at 2. Second, Mr. Chatrie's phone shows that Google Assistant was installed two minutes earlier, at 4:06:51 UTC. A Google "Audit Log" shows three timestamps indicating changes to the Location History setting occurred just seconds later at 04:07:25 UTC, 4:09:08 UTC, and 04:09:08 UTC. *See* Def. Ex. 6 at 4. Therefore, Mr. McInvaille concluded that "it is likely Google Location History was enabled using the Google Assistant application." Def. Ex. 6 at 5. Neither the government nor Google can challenge this conclusion. *See* Tr. 287.

When a user who does not have Location History enabled attempts to use Google Assistant for the first time, Google displays a pop-up box that is part of a "consent flow" that prompts the user to enable up to three Google features, including Location History. This pop-up box will also

appear if the user "long press[es] the home button" on an Android device that does not have Google Assistant set up. Tr. 79; Tr. 351. A "long press" means leaving one's finger on the button for a moment, as opposed to tapping it quickly; the "home button" is the big button at the bottom of the screen. On Android devices like Mr. Chatrie's, a long press of the home button will activate Google Assistant, as if a user had opened the application by tapping on an icon.

Neither Google nor any party has been able to definitively state how this "consent flow" would have appeared on Mr. Chatrie's device on July 8, 2018. Tr. 81, 298. There are two possibilities, however. *See* Def. Ex. 7 at 1–3; Tr. 298. First, the screen could have read: "Creates a private map of where you go with your signed-in devices" with a blue "YES I'M IN" button, as shown below in Figure 3. *See* Def. Ex. 7 at 2. Alternatively, the screen could have read: "Saves where you go with your devices" with a blue "TURN ON" button, as shown below in Figure 4. *See* Def. Ex. 7 at 4; Def. Ex. 23 at 8; Tr. 102, 298. Google calls this line the "descriptive text." Tr. 328. Above both versions of the descriptive text, at the top of the screen, was a sentence that read: "The Assistant depends on these settings in order to work correctly." Def. Ex. 7 at 3. And at the bottom of the screen, separated by a line and in lighter and less-contrasting font, were two additional sentences indicating that this data "may be saved" and that "You can see your data, delete it and change your settings at account.google.com." Def. Ex. 7 at 4; Def. Ex. 23 at 8.

Figure 3

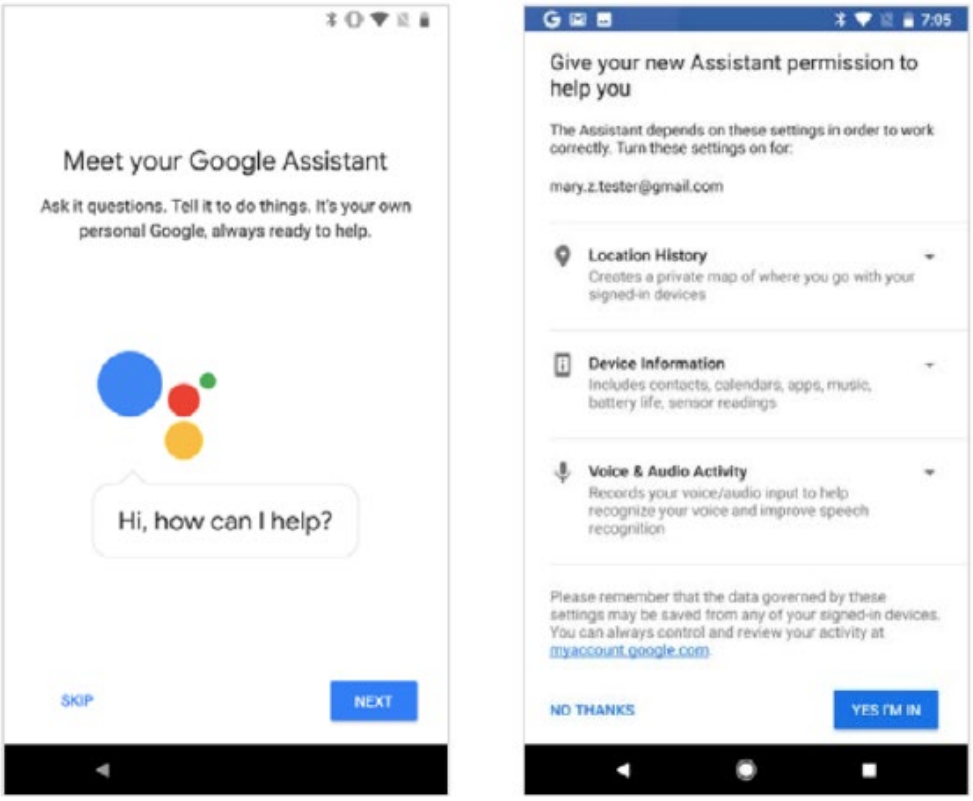


Figure 4

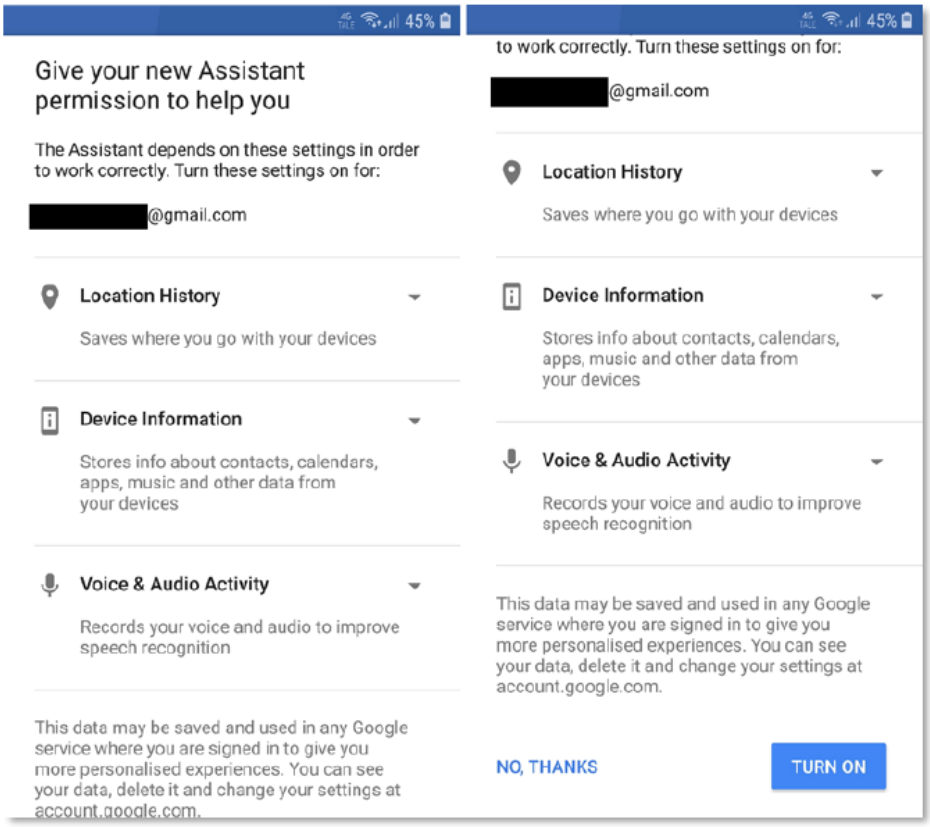
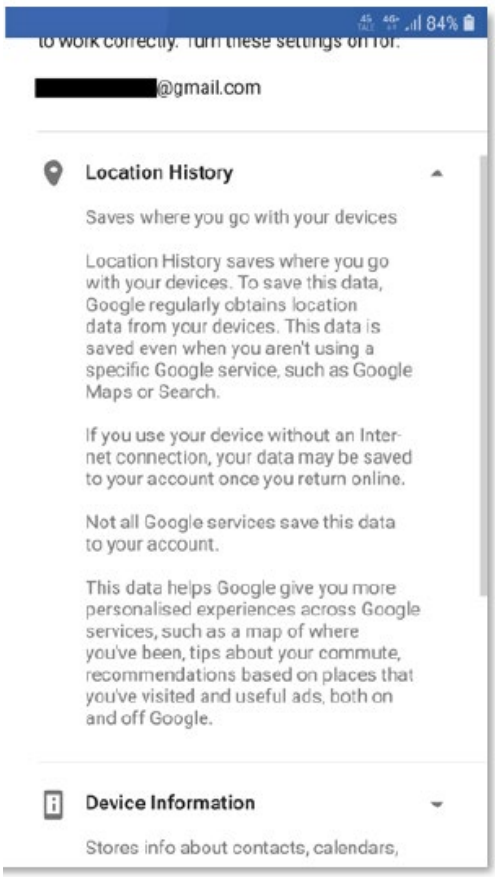


Figure 5



As shown here in Figures 3 and 4, this screen would have asked users to enable two other Google settings—"Device Information" and "Voice & Audio Activity"—if not already enabled. Def. Ex. 7 at 3; Tr. 109, 333. If presented with more than one permission, a user would have had to enable all of them together, or else quit the Google Assistant setup. Tr. 109, 334. In other words, users were not given the option to make an individual determination with respect to each of the three possible permissions. *Id.*

Additional information, which Google calls the "consent copy text," is shown only if users tap on the "expansion arrow," the small triangle on the other side of the page from "Location History." *See* Tr. 106, 329. Figure 5 depicts this "copy text" for Location History, which would have been the same regardless of which "descriptive text" appeared. *See* Def. Ex. 7 at 3; Tr. 271. **Users are not required to view the "copy text."** Tr. 330. Only users who tap the expansion arrow will see it. Def. Ex. 7 at 3; Tr. 110, 345. **And users can enable Location History without ever seeing this information.** *See* Tr. 110, 330, 335.

The Google Assistant setup screen did not contain or link to Google's Privacy Policy. *See* Def. Ex. 7 at 1–4. Users who nonetheless viewed Google's Privacy Policy during the relevant timeframe—from when Mr. Chatrie enabled Location History in July 2018 to his arrest in September 2019—would have seen two different versions of the policy depending on when they accessed it. In the first iteration, in effect from May 2018 to January 2019, the Privacy Policy

mentioned "Location History" twice. *See* Tr. 294. The first reference read: "You can also turn on Location History if you want to save and manage location information in your account." Def. Ex. 43 at 7. The second reference stated: "Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions." *Id.* at 8. The next iteration of the Privacy Policy covered January 2019 to October 2019, and changed the first reference to read: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." Def. Ex. 44 at 7. The second reference remained the same. *See id.* at 8.

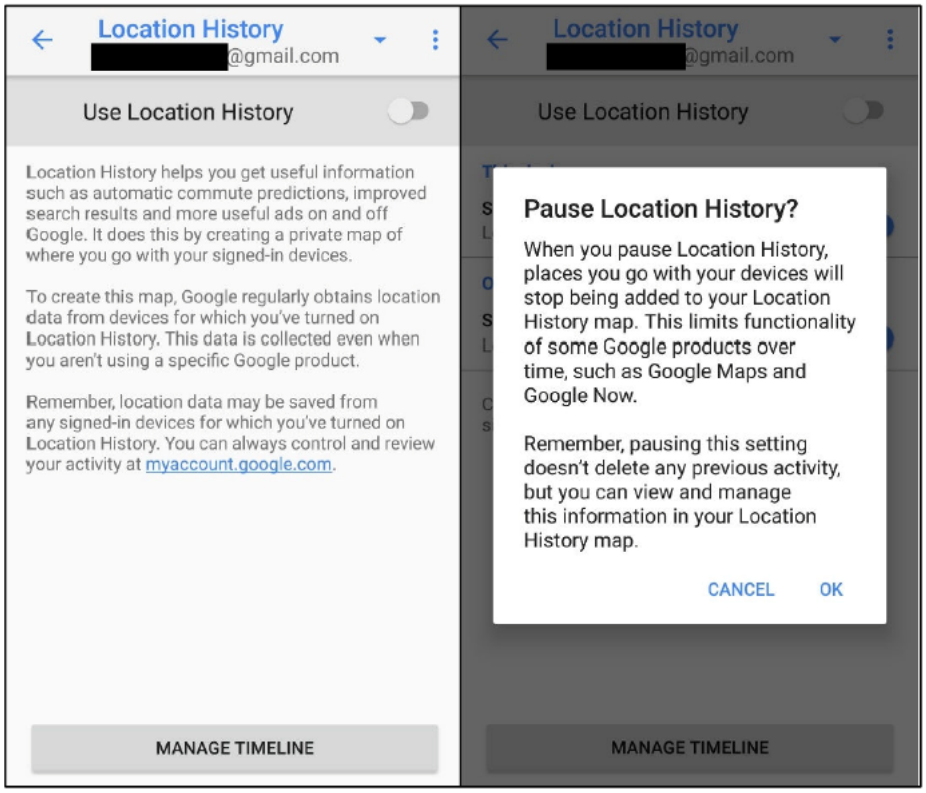
V. "Pausing" Location History

Once enabled, Location History cannot be turned "off," only paused. Tr. 360–61. There are three ways to pause Location History: (1) in the settings for an application like Google Assistant, (2) in the settings panel for the device, or (3) by logging in to "myactivity.google.com" and changing the account's settings. *See* Tr. 340–41. These are the only methods of pausing Location History. **If a user disables or stops using Google Assistant, for example, Location History is still enabled and running**. Tr. 123-24, 362. A user has to know to actively navigate one of these paths in order to locate and pause Location History. Tr. 341. Upon doing so, Google would display another pop-up screen containing text called the "pause copy," as shown in Figure 6. Def. Ex. 27 at 23.

The text of the "pause copy" warns users that pausing Location History will "limit[] functionality of some Google products over time, such as Google Maps and Google Now." It does not specifically mention Google Assistant or provide any details about how app functionality might be limited. In fact, Google Assistant will continue to function with Location History paused, but

Google does not inform users of this option, either when setting up the application or when displaying the "pause copy." *See* Tr. 339, 343.

Figure 6



VI. Deleting Location History

Just as pausing Location History does not delete Location History data, disabling Google Assistant does not delete Location History data. That requires manual input. *See* Tr. 356, 361. Google now offers an "auto-delete" function that allows users to automatically delete Location History data older than three months, *see* Def. Ex. 46, but this function was unavailable for Mr. Chatrie. Tr. 356. To delete Location History data manually, a user must access the "Timeline UI," or user interface, at which point records can be deleted by day or date range. Tr. 356. Deleting Location History records will not stop Location History from continuing to collect data. Tr. 188.

VII. The Geofence Warrant

The warrant in this case authorized the search of all Google Location History data, for all users, in order to identify devices of interest and obtain additional information about those accounts. The warrant outlines a dependent, three-step process, now familiar to this Court. *See* Def. Ex. 2 at 12–14; *see also* ECF No. 29 at 4–7; ECF No. 104 at 1–2.

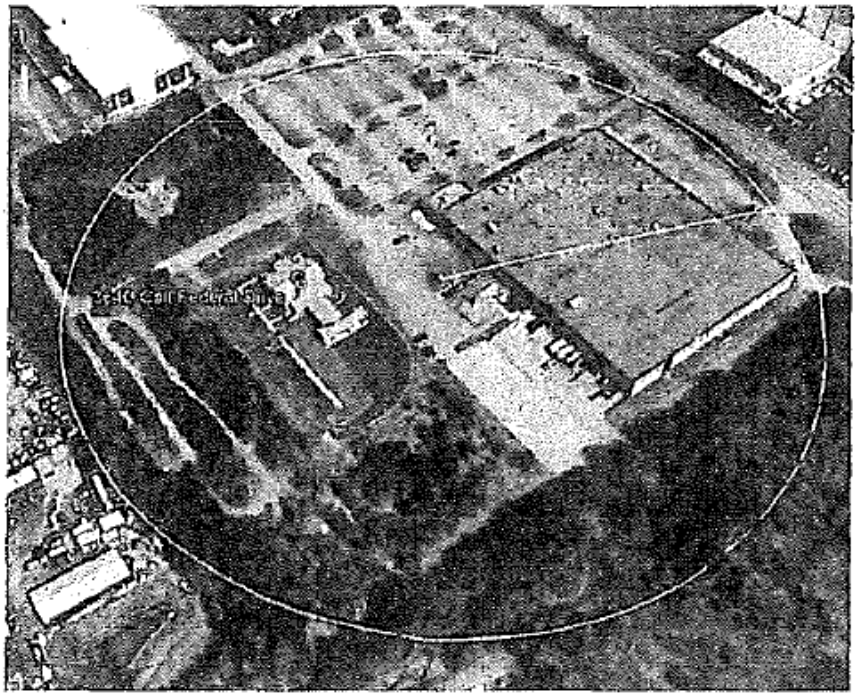
Step one required Google to search the Sensorvault to determine which devices were purportedly within 150 meters of the Call Federal Credit Union during the time of the robbery as well as 30 minutes before and after it occurred. Def. Ex. 1 at 4. To carry out this command, Google had to search the contents of every account with Location History enabled, *i.e.*, "numerous tens of millions" users, for records satisfying the government's criteria. Tr. 29, 52–53, 204–05. It is impossible to search only users who were within 150 meters of the bank because there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." Def. Ex. 2 at 12. Rather, "Google must search across all Location History journal entries to identify users with potentially responsive Location History data, then run a computation against every set of coordinates to determine which Location History records match the time and space parameters in the warrant." Tr. 204 (quoting Def. Ex. 2 at 12).

Google ultimately identified 19 accounts with responsive data. The government seized those records in a database file containing 210 location points on June 28, 2019. Tr. 132, 642. Google states it provided this data in "anonymized" form, meaning that it did not include account names or usernames. Tr. 404. It did, however, contain a "Device ID" number, a unique number in Sensorvault linked to the user's device that does not change over time. Tr. 451, 453–54.

Google identified this data by selecting any devices with an estimated latitude/longitude inside the 150-meter geofence from the warrant, shown in Figure 7. For some of these location

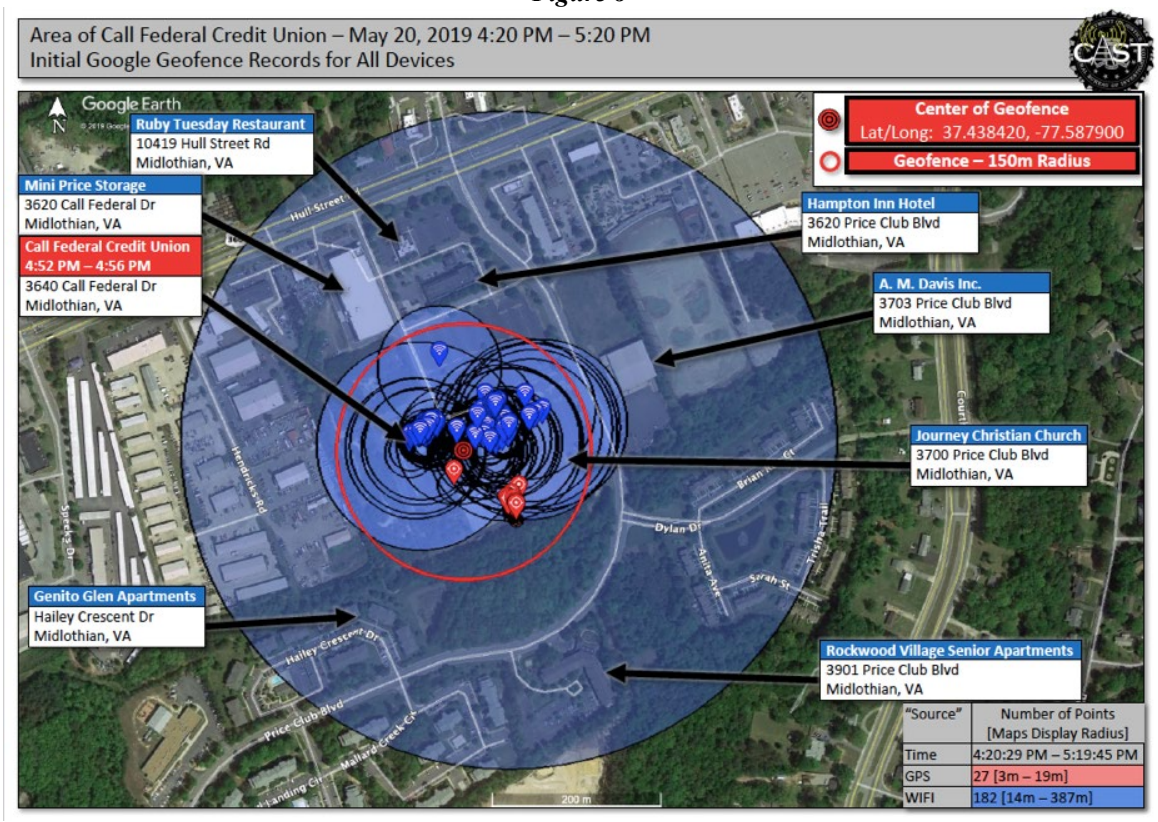
points, however, the Map Display Radius extended beyond the geofence, meaning that the device was just as likely to be outside the boundary. *See supra* at 7; Tr. 587–88. Both Google and the government acknowledge this possibility of "false positives." *See* Tr. 586; Def. Ex. 2 at 9, 20 n.12.

Figure 7



The largest Display Radius is 387 meters from coordinates near the center of the 150-meter geofence. *See* Def. Ex. 3 at 6–12, 17–37. Consequently, the effective range of the search was more than twice as far as the geofence requested in the warrant. Tr. 41–42. Agent D'Errico notes that the actual location of that device remains unknown, meaning that it could have been inside or outside the geofence. *See* Tr. 587. All agree, however, that there is a 68% chance it was somewhere in the largest blue circle depicted in Figure 8 below. Tr. 39–40, 215, 587. That circle encompasses not just the bank and the Journey Christian Church, but also multiple streets plus all of the businesses and residences nearby—including Hull Street and Price Club Drive, Ruby Tuesday's, the Hampton Inn, A.M. Davis, Inc., Mini Price Storage, the Genito Glen Apartments, and the Rockwood Village Senior Apartments. *See* Tr. 32–33, 49; 1/21/20 Tr. at 66–67.

Figure 8



Step two of the warrant process required the government to review the step one data and "attempt to narrow" the list of devices. Def. Ex. 1; Tr. 592. Google would then provide two hours of additional Location History data for a subset of those devices, called "contextual" data, for one hour before and after the robbery. *Id.*; Tr. 26, 30.

Initially, Det. Hylton sent two emails on July 1 and 2, 2019, each requesting contextual data for all 19 devices from step one. *See* Gov't Ex. 4; Tr. 472, 622; ECF No. 96-2 at 5. Det. Hylton also requested the subscriber information for all 19, *i.e.*, "de-anonymized" records that the warrant reserved for step three. *Id*. Det. Hylton sent these emails after consulting with the United States Attorney's Office. Tr. 622. When Det. Hylton did not receive a reply from Google, he left two voicemails on July 8, 2019. Tr. 621–22, 642. A Google specialist called back the same day and specifically advised Det. Hylton that the warrant required the government to narrow the number of devices for which they were seeking expanded data. Tr. 473–74. Google did not say by how

much the government had to narrow the list, but advised it was required. *Id.* at 474. The Google specialist also had to advise Det. Hylton about what types of information would be produced in the later stages of warrant. *Id.* The specialist reported to her supervisor, Ms. Rodriguez, that it did not appear Det. Hylton was familiar with the process outlined in the warrant. Def. Ex. 24 at 5-6.

Following the July 8 phone conversation with Google, Det. Hylton emailed Google once again, this time requesting stage two data (only) for nine of the 19 devices. Tr. 642. Accordingly, Google created another database file on July 9, 2019, containing the "contextual" data for those nine devices and sent it to the government. *See* Def. Ex. 8.

Step three of the warrant required the government to further cull the number of devices and identify an even narrower subset. Tr. 26, 543–44; Def. Ex. 1. Google would then produce de-anonymized account information, including the username and subscriber information, associated email addresses and telephone numbers. *Id*. The government twice requested this data for three devices on July 10 and 11, 2019. Tr. 643. On July 11, Google sent the government a third database file matching each "Device ID" with its "Gaia ID" as well as records reflecting the associated subscriber information. Tr. 544. One of those three subscribers was Mr. Chatrie.

ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie's reasonable expectation of privacy in his Google data. For the reasons set forth below, Mr. Chatrie maintains that the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16–24; ECF No. 104 at 10. The *Leon* good faith doctrine does not apply because the warrant was so obviously deficient that it was *void ab initio*. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

I. Mr. Chatrie Had a Reasonable Expectation of Privacy in His Location History Data.

Mr. Chatrie enjoys a reasonable expectation of privacy in his Location History data following the Supreme Court's landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012). Although the shortest search at issue in either case involved seven days of cell phone location information for a single individual, *see Carpenter*, 138 S. Ct. at 2217, the Court's reasoning applies with at least equal force here. *See* ECF No. 104 at 10; ECF No. 29 at 9.

A. Location History Is At Least As Precise as CSLI

Location History data is at least as precise as the CSLI in *Carpenter*. *See* ECF No. 104 at 12–14. The government concedes this point. *See* ECF No. 41 at 8; ECF No. 109 at 9. In this case, all of the estimated Location History points derive from either Wi-Fi or GPS signals, which Google states are "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." Def. Ex. 21 at 4. Additionally, 12% of the data points in this case are from the same type of GPS signals at issue in *Jones*, which can be accurate to less than a meter. *See* Tr. 18–20; ECF No. 29 at 8; ECF No. 104 at 14.

But, Google did not design Location History to solve bank robberies. Google's estimation of a device's location may be "sufficiently precise and reliable for the purposes for which it was designed," *i.e.*, creating a user Timeline and targeting advertisements within a kilometer. Def. Ex. 2 at 10 n.7.; *see also supra* at 8. But because Google did not design Location History to respond to 150-meter geofence warrants, its ability to accurately do so comes with caveats, such as the possibility of "false positives," *see supra* at 8, 17, and "false negatives." *See* Tr. 44–45, 47–48, 217, 585. Also, due to the Map Display Radius, the effective range of the search extended more than twice as far as the 150-meter circle described in the geofence warrant. *See supra* at 17.

B. A Search of Location History Data Is Highly Intrusive

A search of even small amounts Location History data is highly intrusive. As the government recognizes, *Carpenter* "explicitly declined to determine whether there is a 'limited period' for which the government can acquire cell phone location information without implicating the Fourth Amendment." ECF No. 41 at 7. Short-term searches are capable of revealing the "privacies of life," 138 S. Ct. 2214, which was the Court's main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called "long-term" searches,[5] what motivated the Court in each instance was the risk of exposing information "the indisputably private nature of which takes little imagination to conjure: 'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'" *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009)); *accord Carpenter*, 138 S. Ct. at 2215. Thus, "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance … will require particular attention." *Jones*, 565 U.S. at 415. The same is true for cell phone location information, given that "[a] cell phone faithfully follows its owner beyond public throughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Even before *Jones* and *Carpenter*, the Supreme Court was concerned with short-term location tracking, especially when it reveals information about the interior of a constitutionally-protected space, such as a home. In *United States v. Karo*, the Court found that using an electronic beeper to track an object inside a private residence was a search. 468 U.S. 705, 716 (1984). A

[5] In fact, the government's demand for seven days of data in *Carpenter* netted only two days of data. *See* 138 S. Ct. at 2212.

search occurs at the moment the object "has been withdrawn from public view." *Id.* at 717. Especially relevant here, the Court remarked that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *Id.* at 716. So too in *Kyllo v. United States*, the Court found that using a thermal imaging device to peer through the walls of a private residence was a search. 533 U.S. 27, 37 (2001). It was a search despite the fact that the scan "took only a few minutes" and could not show people or activity inside. *Id.* at 30. As the Court explained, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Id.* at 37.

Here, the geofence search revealed Google users inside the bank as well as in nearby homes, apartment complexes, a hospital, and the Journey Christian Church. *See* 1/21/20 Tr. at 80–90 (describing the paths for "Mr. Green," "Mr. Blue," and "Ms. Yellow"). Although Google had "anonymized" this data, the defense was easily able to determine the likely identities of at least three individuals. *See* Tr. 62–70; ECF No. 104 at 12; 1/21/20 Tr. at 83, 87–88, 90–91. This is why Google treats Location History data not as a "business record" but as sensitive user "content" under the Stored Communications Act, 18 U.S.C. § 2703, likening it to a "digital journal" of users' movements and travels and requiring a warrant to search it, even for two hours of data. *See* ECF No. 104 at 12; Def. Ex. 2 at 16. Furthermore, once the government seizes the "anonymized" Device IDs in steps one and two, it could simply obtain the subscriber information for any Device ID by issuing a subpoena to Google. In Illinois, Judge Fuentes recently denied a geofence warrant application in which the government promised to forego step three, finding that there is "no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber

identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities." *See* Fuentes Opinion, 481 F. Supp. 3d at 754.

Focusing only on the length of the search, however, is to ignore the unprecedented breadth of a geofence warrant, setting it apart from the individualized searches in *Jones* and *Carpenter* (and most every other case). This was not a search of one person's data over the course of one or two hours; it was a search of "numerous tens of millions" of people, all at once.

The government argues that this defining feature of a geofence warrant is irrelevant to the Fourth Amendment analysis, *see* ECF No. 109 at 8. But as Justice Gorsuch remarked, "On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" *Id.* at 2267 (Gorsuch, J., dissenting). The fact that the government is searching millions multiples the privacy intrusion.

C. Mr. Chatrie Did Not "Voluntarily" Share Location History Data With Google

The government contends that Mr. Chatrie has no expectation of privacy in his Location History records because Location History is an "opt-in" service and he "voluntarily" shared this data with Google. *See* ECF No. 109 at 5; ECF No. 41 at 10–12. But Mr. Chatrie maintains that, as in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745). But based on the facts in this case, it is clear that typical users like Mr. Chatrie would have no idea what Location History is, how it works, or whether they have it enabled on their phones.

An examination of the "opt-in" process reveals that the act of enabling Location History could not have been meaningful or informed, but was perfunctory at best and deceptive at worst.

This is evident on its face from the evidence presented to this Court about how the "consent flow" pop-up screen appears in Google Assistant. *See supra* at 11–13. It is also bolstered by the highly public and highly negative "feedback" that Google received regarding Location History and consent, reflected in changes that Google made to Location History after the facts of this case. And it is further demonstrated by the words of Google's own engineers, who repeatedly emailed a massive, company-wide discussion group to express their frustration over Google's lack of clarity with respect to location tracking permissions, and with Location History specifically.

First, consider the "opt-in" process. Google describes it as a complex seven-step process. Def. Ex. 2 at 7–8; Def. Ex. 21 at 2–3. But for Mr. Chatrie, it boiled down to a single pop-up screen in Google Assistant, at midnight, a week after he got the phone. *See supra* at 10.[6] That screen had one phrase of "descriptive text" about Location History. It in no way indicated that location data would be saved by Google, as opposed to stored locally on the device. It did not begin to convey the fact that it would operate independently of Google Assistant or convey that Google would collect location data constantly, at an average of every two minutes. *See supra* at 5. While additional information was available, users would have had to actively seek it out. Even then, what little else Google said about Location History did not adequately convey how it functioned.

There is a vast chasm between the reality of Google's Location History data collection and the advisements it actually requires users to read. To begin with, the "descriptive text" for Location History—the only text a user is actually required to read—is not only inadequate but outright confusing. One iteration tells users that it "Creates a private map of where you go with your signed in devices." *See supra* at 11. A later version says that Location History "Saves where you go with

[6] Previously, counsel for Mr. Chatrie suspected that the opt-in to Location History occurred either during the initial setup of the device, or upon opening an application like Google Maps. *See* ECF No. 104 at 15–18; Def. Ex. 21 at 2–3; Def. Ex. 2 at 12.

your devices." *See id*. In either event, a user might reasonably infer that this "private map" or saved data would be saved only on their device, not with Google. Tr. 301, 346 (descriptive text does not make a "distinction" as to whether location information is saved on-device or on Google servers).[7] In fact, that is how certain personalized features work on Apple Maps, available on Apple iPhones. *See Privacy*, Apple, https://www.apple.com/privacy/features/ (last visited Apr. 23, 2021) (describing how certain personalized features on Apple Maps "are created using data on your device" to "help[] minimize the amount of data sent to Apple servers"). Unless a user actively clicked the small "expansion arrow" on the other side of the screen from "Location History," there would be no indication that the data is saved in the cloud on Google's servers. *See supra* at 13; Tr. 110, 330. Google does not maintain records on who or how many people click the expansion arrow, Tr. 365, and there is no indication that Mr. Chatrie did here.

Additional language appeared at the bottom of the screen, away from the Location History "descriptive text," and in lighter font. There are two potential versions of this language, *see supra* at 11-12, but both state that this "data may be saved" and that "You can see your data, delete it and change your settings at account.google.com." *Id*. Neither version mentions Location History or location data, nor gives any indication of what it is, let alone that the phone will begin to transmit its location to Google every two minutes in perpetuity. It does not mention the Location History "Timeline," the virtual "journal" that is supposedly the reason users enable Location History.

Google did not require users to view any other text before enabling Location History, Tr. 110, 330, and, the other optional information it provided did not put users on notice about the true nature of the Sensorvault database. The expanded "consent copy," for instance—viewable only if a user clicked on the expansion arrow near "Location History"—explained that Google would

[7] Mr. McGriff testified that Google does not ascribe any significant difference in meaning between these two variations, s*ee* Tr. 301, raising the question of why the change occurred at all. *See infra* at 35.

obtain location data from users' devices, but it contained no warning about the frequency or sheer quantity of data collected. Tr. 347–48; *see* Def. Ex. 7 at 3. In this case alone, the Location History records revealed that Google collected location information every six minutes, twenty-four hours a day, seven days a week. Tr. 122, 436. On average, Google collects Location History data as often as every two minutes. *See supra* at 5. Nothing in the "descriptive text" or the "consent copy" explains the volume of information that Google plans to collect.

Additionally, nothing explains that Location History will operate independently, regardless of whether the phone is in use. The government contends that Mr. Chatrie's "voluntary disclosure of location information to Google is evident from the nature of the location-based services (like mapping) that Google provided him." ECF No. 109 at 9–10. But this argument falls flat. Once enabled, Location History silently collects data in the background, regardless of what a user is or is not doing on the device. This is in stark contrast to the facts in *Smith v. Maryland*, where phone users often had to interact with telephone operators using switching equipment to complete calls. *See* 442 U.S. 735, 742 (1979). Here, Mr. Chatrie could have enabled Location History by accident, just after midnight, following a long-press of the home button, after a week of annoying prompts, on a pop-up screen for Google Assistant, and bundled with other choices. If he did this, there would still be no further indication that Location History was running. Even if Mr. Chatrie never again engaged with Google's "location-based services," or any other Google service, Location History would be enabled and tracking his location at all times, even while he slept. *See supra* at 5; Tr. 122 ("[T]here were no periods of data not being collected.").

Google's Privacy Policy has little if any bearing on an individual's Fourth Amendment expectations of privacy. *See United States v. Irving*, 347 F. Supp. 3d 615, 621 (D. Kan. 2018) (rejecting government's argument that defendant had no expectation of privacy in his Facebook

account information where he agreed to Facebook's terms that "generally inform[ed] users that Facebook collects a user's content and information."); *see also Smith*, 442 U.S. at 745 (declining to "make a crazy quilt of the Fourth Amendment" based on phone company policies). It is of no assistance to the government here. First, there is no link in the "consent flow" at issue to Google's Privacy Policy, *see* Def. Ex. 7 at 1–4, a factor that courts weigh heavily when evaluating reasonable notice. *See* ECF No. 104 at 18–20; *Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *9 (E.D. Va. Jan. 28, 2020). Second, the text of the policy was not any more illuminating than the pop-up screen. *See supra* at 19. At the time Location History was enabled on Mr. Chatrie's phone, the policy had just two lines that mention Location History. *See* Tr. 294. One line cast Location History only as a way to "save and manage location information in your account." Def. Ex. 43 at 7. The other line, in passing, states that "you can turn on Location History if you want traffic predictions for your daily commute." *Id.* at 8. These brief mentions sow only further confusion.

The government likes to point out that it was still possible to disable Location History and delete saved records. *See* Tr. 160, 416. But this assumes that Mr. Chatrie was both fully aware of the collection taking place as well as knowledgeable about how to control or stop it, and the government has offered no evidence to indicate that this was the case. On the contrary, while it is arguably too easy to enable Location History, it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete, assuming he even knew about its existence.

Deleting the application from which Location History was enabled, for example, would not turn off Location History. Tr. 124; *see* Tr. 361–62. Likewise, deleting Location History data would not turn off Location History. Tr. 361. Indeed, it is telling that, once enabled, Location History can never be turned "off," only "paused." *See supra* at 14. And it is only possible to "pause" Location History by navigating through complicated settings menus and disregarding a

pop-up warning from Google that doing so will "limit[] functionality" on the device. *See id*. Similarly, while pressing "pause" means that no future data will be recorded, it does not delete any past data collected. *See supra* at 15. Even disabling Google Assistant, the app used to enable Location History here, would have no effect on either stored data or future collection. *See id*. In short, for a user to completely remove their data from the Sensorvault database, they would need to follow a specific settings permutation: a two-step process of both deleting all past Location History data and "pausing" Location History. Nowhere, not in either version of the "consent flow" or the Privacy Policy, did Google inform users of the need to take both steps or how to do them.[8]

This is not surprising, however, because Google has a clear financial incentive in increasing the number of users with Location History enabled. *See supra* at 8–9; Tr. 435–36. Google is not disinterested or neutral when presenting users with options. Rather, Google is invested in having users whose data can be used to sell lucrative advertisements that calculate rate of return by measuring "store visits." *Id*.; Tr.196–97, 301. Indeed, advertising is the main "product" that drives Google's revenue. *See* Tr. 560; *see also* Gov't Ex. 1 at 40 (showing that advertising comprised 85% of Google's revenue in 2018). In this light, the "consent flow" fits the pattern perfectly and bears a striking resemblance to lobster traps: easy to get in, hard to get out.

At the same time, Google has never been immune to public criticism, lawsuits, or regulatory action. On the contrary, Google has repeatedly received terrible headlines, civil complaints, and government inquiries over its location tracking practices, putting the company

[8] Instead, media outlets have taken on this task, publishing "how-to" articles on disabling Location History and other forms of Google location tracking. *See*, *e.g.*, Dave Johnson, *How to Stop Google from Tracking Your Android's Location*, Business Insider (Nov. 25, 2020, 9:16 AM), https://www.businessinsider.com/how-to-stop-google-tracking-android; Barbara Krasnoff, *Android 101: How to Stop Location Tracking*, Verge (Aug. 25, 2020, 3:04 PM), https://www.theverge.com/21401280/android-101-location-tracking-history-stop-how-to; Chandra Steele & Jason Cohen, *How to Get Google to Quit Tracking You*, PC Mag (Feb. 11, 2020), https://www.pcmag.com/how-to/how-to-get-google-to-quit-tracking-you; Todd Haselton, *Google Maps Tracks Everywhere You Go. Here's How to Automatically Delete What It Stores*, CNBC (Dec. 7, 2019, 9:15 AM), https://www.cnbc.com/2019/12/07/how-to-stop-google-maps-from-tracking-your-location html.

squarely on notice that its practices surrounding user consent were unacceptable and incompatible with user expectations of privacy. And in response, Google acted. *See* Def. Ex. 46; Def. Ex. 47; Tr. 260, 317, 383. Although, Google notes that it is "always looking for ways to further improve," Tr. 300, the changes Google made to Location History in this context are telling.

Since at least 2017, Google has been on notice that people found it difficult to understand how Google collects location data and what their options are. Mr. McGriff, in charge of Location History for Google since 2016, *see* Tr. 192, was acutely aware of a 2017 article in the online magazine *Quartz* as well as a 2018 article by the *Associated Press* ("AP"), both involving Location History. Tr. 220, 223–24. Both articles described Location History with alarm and were highly negative. Tr. 221–23, 225–26. The AP article made such an impression that Google prepared a report tracking how much follow-up coverage mentioned the "lack of user consent/creepy factor." Tr. 228. It also became the subject of a Monday-morning "Oh Shit" meeting for the Location History team. Tr. 248. In his defense, Mr. McGriff noted that the Google Location History team has such a meeting every Monday, which is understandable. *See id.*

It is understandable because those articles were just the beginning of the public "feedback" that Google received regarding Location History and Google's location tracking practices. *See* Tr. 218–19. Google not only became aware of the *Quartz* article, for example, but also the subsequent letter that the United States Senate to the Federal Trade Commission, urging the agency to investigate "deceptive acts and practices" associated with Location History. *See* Tr. 236; Def. Ex. 53 at 4 ("Most consumers do not understand the level, granularity, and reach of Google's data collection, and there are serious questions about whether they have provided their informed consent and maintain a reasonable ability to avoid participating in this collection."). And following the 2018 AP article, Google became aware of a class action lawsuit over its location tracking

practices. *See* Tr. 236–37. Google was also aware of a *New York Times* article revealing Google's role in geofence warrants, which in turn prompted another letter critical from Congress (this time addressed to Google's CEO). *See* Tr. 314.

Most recently, the Attorney General of Arizona filed lawsuit against Google, leading to the public release of hundreds of pages of internal emails concerning Location History. *See* Tr. 240. After publication of the AP and *Times* articles, Google employees took to company-wide email groups to express their confusion over Google's location settings. *See*, *e.g.*, Tr. 241–43, 246, 252–53, 255–56; Def. Ex. 30; Def. Ex. 31 ("Add me to the list of Googlers who didn't understand how this worked and was surprised when I read the article."); Def. Ex. 36 (explaining that Google was "trying to rein in the overall mess that we have with regards to data collection, consent, and storage"); Tr. 310–12; Def. Ex. 37 ("I'd want to know which of these options (some? all? none?) enter me into the wrongful-arrest lottery. And I'd want that to be very clear to even the least technical people.").

Regardless of the truth of these criticisms, there is no question that Google heard, discussed, internalized, and then acted on them. Public reaction was strong enough that Google made reforms to Location History, crediting this "feedback" for spurring the "auto-delete" option for Location History data. *See supra* at 15; Tr. 317; Def. Ex. 46. Google also began to send out monthly emails to users who had enabled Location History, after recognizing that users might not "understand the granularity of the data that's being collected or simply just wouldn't know . . . what exactly [Google was] collecting and how that information was being processed." Tr. 359–60. Google has no record of sending such emails to Mr. Chatrie and concedes that it may not have

sent him those emails.[9] Tr. 328; Def. Ex. 23 at 8–9. Nonetheless, these changes demonstrate that even Google knew that the "opt-in" for Location History was confusing and potentially deceptive.

D. The Third-Party Doctrine Should Not Apply Even If Mr. Chatrie Intentionally Enabled Location History.

Timothy Carpenter signed a contract with his cell phone service provider. *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting). He did not allege that he was tricked or coerced into it. And yet, the Supreme Court still found that he was not "voluntarily" conveying his location data to the service provider, even though everyone was aware that that is how cell phones work. *Id.* at 2220 ("Cell phone location information is not truly 'shared' as one normally understands the term."). Rather than "mechanically" applying the third-party doctrine, the Court looked at the context—whether the "choice" to hand over the data truly outweighed the privacy intrusions given the realities of the digital age. *Id.* at 2219–20; *see also* ECF No. 29 at 9–11.

The Court's contextual concern exists here in abundance. "[M]echanically" applying the third-party doctrine here would divest, at a minimum, tens of millions of people of their Fourth Amendment rights merely for participating in normal everyday life. *See* Tr. 205. Google Location History may not be a pillar of digital society, but there are still "numerous tens of millions" of people who use it, wittingly or not. The *Carpenter* Court remarked on the pervasiveness of cell phones in the United States. 138 S. Ct. at 2220 (citing *Riley v. California*, 134 S. Ct. 2473, 2484 (2013)). At issue here is one-third of all Google users. It would be nonsensical to deem this data unworthy of Fourth Amendment protection unless everyone is using it, yet that is the line the government seeks to draw. Moreover, there is nothing in the government's reasoning that would limit the use of geofences to Location History data.

[9] Google also describes a "warm welcome" notification appearing in the Google Maps application, Tr. 355, but there is no indication that there was such a notification in Google Assistant, or that Mr. Chatrie received one.

Under the government's theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI. Thus, there would be nothing separating a search of Location History data from a search of Gmail users for messages mentioning a robbery of the Call Federal Credit Union. This is no mere hypothetical. Law enforcement has already forced Google to conduct reverse "keyword" searches, disclosing everyone who searched for a particular term or address.[10]

Lastly, Mr. Chatrie respectfully persists in his property-based arguments here. *See* ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21. Ownership is inherent in the language Google uses to describe Location History, whether telling users they are creating a "private map" of their whereabouts or calling it "your data" to delete or manage as users see fit. *See supra* at 11. Under either a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, obtaining Mr. Chatrie's Google Location History records was a Fourth Amendment search.

II. The Geofence Warrant Was an Unconstitutional General Warrant

As Mr. Chatrie has argued from the beginning, geofence warrants are inherently unconstitutional. *See* ECF No. 29 at 19–21; ECF No. 104 at 21. They are digital versions of the "dragnet" searches that Fourth Amendment was intended to prohibit. *See* ECF No. 104 at 21–24; ECF No. 29 at 16–23. The Supreme Court has never sanctioned the search of "numerous tens of millions" of people, in any context. *See* Def. Ex. 21 at 4. Additional facts from the March hearing confirm that the warrant in this case was uniquely overbroad and so lacking in particularity that it is the digital equivalent of an impermissible general warrant.

[10] Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020 1:21 PM), https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/.

E. Overbreadth

Overbreadth concerns probable cause, which is defined as "a fair probability" that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A warrant is overbroad if the government lacks probable cause for the things to be searched or seized. *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). Here, the government did not have probable cause to search "numerous tens of millions" of Google accounts. It did not have probable cause to search 19 users, either, and it did not have probable cause to search nine or three. The government did not have probable cause to search even one Google account, because investigators admittedly had no suspects. Tr. 487, 637. No matter how the government seeks to dress it up in steps or stages, the complete absence of probable cause means that the warrant is fatally overbroad from beginning to end.

Step one was a dragnet, conducted by Google at the government's direction. The government made Google search through every user account with Location History enabled to identify any people within 150 meters of the Call Federal Credit Union during a 1-hour window. According to Google, this required searching "numerous tens of millions" of accounts—reviewing the contents of each one to determine if it met the government's criteria. Tr. 29, 52–53, 205; *see* Tr. 575. In other words, the government compelled Google to access "numerous tens of millions" of accounts and apply a filter of the government's peculiar design—a digital dragnet.

The warrant application provided no case-specific facts that the robber was a Google user or had Location history enabled at the time in question.[11] All the government offered was that an unknown bank robber had a cell phone and that Google tracks a lot of people's cell phones. ECF

[11] Despite "tens of millions" being an exceedingly large number, it accounts for only one-third of Google's active users. In other words, even if every cell phone user was signed into a Google account, there would only be a one in three chance of the suspect having LH enabled.

No. 109 at 14. The government contends that this is a "substantial basis" for probable cause, *id.*, but if that is true, then the government could get a geofence warrant in any investigation, simply by reciting the facts of the crime and some statistics about Google. As Mr. Chatrie has consistently argued, such broad conjecture about the popularity of Google or cell phones generally does not amount to probable cause. *See* ECF No. 29 at 23; ECF No. 48 at 19. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). In Illinois, Judge Fuentes denied the government's application for a geofence warrant on these grounds, noting that it "resembles an argument that probable cause exists because those users were found in the place … [where] the offense happened," an argument the Supreme Court squarely rejected in *Ybarra*. *See* Fuentes Opinion, 481 F. Supp. 3d at 754.

Had the government provided a nexus between the robber and Location History, then there would have been no need to go fishing in Google's ocean of data. The government could have simply requested the Location History data for the suspect account, as it typically does. But, the government did not seek to search a particular account; it sought to search *all* accounts. That is the definition of a general warrant. *See Warden v. Hayden*, 387 U.S. 294, 313 (1967) (describing the "practice of the Star Chamber empowering a person 'to search in all places, where books were printing, in order to see if the printer had a licence; and if upon such search he found any books which he suspected to be libellous against the church or state, he was to seize them, and carry them before the proper magistrate.'").

The fact that the government's dragnet ensnared 19 people does not diminish the scope of the initial search conducted at their behest. The Fourth Amendment does not distinguish between Google and the government when it comes to conducting this initial search of millions. This case does not involve a "private search." Google did not decide on its own to search for users near the

bank, and Google never provides such information to advertisers. *See supra* at 9; Tr. 432–33. Likewise, the data produced was not an existing "business record." Google did not possess a list of people near the bank until the government required them to create one. Tr. 433. In short, Google had no independent motivation to conduct this geofence search, and Google would not have done so without a warrant. *Id.* The entire search, including the "numerous tens of millions" in step one, was conducted at the government's direction.

The government contends that this was just like a "tower dump"—another type of exceedingly broad search, the constitutionality of which is in doubt following the Supreme Court's decision in *Carpenter*. A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* Tr. 49–50; Def. Ex. 2 at 14. Any similarity to geofence warrants, however, is merely superficial. Significantly, the number of people searched in a geofence warrant is far larger—by at least four orders of magnitude—than the number of people searched in a typical tower dump. *See* Tr. 53 (the number of people searched in a tower dump "wouldn't be close to" the number of people searched here); *see also* ECF No. 104 at 22 (surveying reported tower dump cases and finding that they tend to impact hundreds or thousands of people at most). Even the government's own hypothetical tower dump would have involved a search of roughly 3,000 people, Tr. 55, which is just a tiny fraction of the "numerous tens of millions" searched here. And more importantly, it is a long way off from a "normal Location History request for a specific account when they name the account because we know who we're looking for." Tr. at 53.

A tower dump is more limited than a geofence, relatively speaking, because cellular service providers organize, or "index" data based on location, *i.e.*, the cell towers in their networks. Unlike Google, they keep information about the use of each tower for internal business purposes, like

identifying towers that become overloaded and determining where to put up more. As a result, they are able to provide information about particular towers without searching the phone records of every customer. Google, on the other hand, indexes Sensorvault by Google account and has no way of searching by location. *See* Tr. 431–32, 572–73. The government responds that they cannot be responsible for the way Google chooses to structure its database and suggests that Google could "create an additional Location History database indexed by location" to make it easier to execute geofence warrants. ECF No. 109 at 17. But Google does not operate cell towers and has no business need to index user data in this way.

Furthermore, the warrant would still be overbroad even if it were somehow possible to restrict the initial search to devices within the geofence. The government argues that the warrant was "limited based on location, dates, and times," but the location at issue is anything but narrowly tailored. It encompasses not only the bank and parking lot, but the entire church nearby, with an effective range that included major streets, a hotel, a restaurant, other businesses, and two apartment complexes. *See supra* at 17-18. Judge Weisman recently reached this conclusion as well in denying the government's application for a geofence warrant in Illinois. *See* Weisman Opinion at *5 ("[T]he geographic scope of this request in a congested urban area encompassing individuals' residences, businesses, and healthcare providers is not 'narrowly tailored' when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation."). Furthermore, the government would not have had probable cause to search all 19 people who happened to be in the area. As Judge Fuentes reasoned, that data might "*include* evidence of the crime, but it will include other information as well: The location information of persons not involved in the crime." Fuentes Opinion, 481 F. Supp. 3d at 751. To justify such an "all persons" warrant, the government would have needed probable cause

that all 19 people were involved in the bank robbery. *See Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) ("[A]n 'all persons' warrant can pass constitutional muster if the affidavit and information provided to the magistrate [judge] supply enough detailed information to establish probable cause to believe that all persons on the premises at the time of the search are involved in the criminal activity."). That would have been impossible to do, of course, because the government would have had no way of knowing, *ex ante*, that there would be 19 people in the geofence.

The fact of the matter remains, however, that the step one search did not just involve 19 people, but "numerous tens of millions," none of which the government had probable cause to search. Probable cause was still absent in steps two and three, when the government seized even more Location History data from nine accounts as well as subscriber information for three of them. *See supra* at 18-19. While the government may have learned new information from the step one data it seized, the warrant application did not change and the government did not seek additional court authorization. The government lacked probable cause to search anyone's Location History, whether three, nine, nineteen, or millions. The warrant was therefore overbroad from start to finish.

F. Particularity

Particularity concerns officer discretion. Warrants must particularity describe both the place to be searched and the items to be seized in order to limit officer discretion and prevent the "exploratory rummaging" that the Framers abhorred. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010). The particularity requirement takes on special importance where, as here, a search implicates First Amendment concerns. *See* ECF No. 104 at 24; ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. In this case, the place to be searched is the millions of accounts stored on Google's servers. The items to be seized are not specified, but instead described as the product of a three-step process that explicitly requires

the government to use its discretion. In reality, the warrant left the entire process up to Google and the government to work out internally.

The basic contours of the warrant were the product of repeated engagement between the FBI and Google. *See supra* at 4. Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data. *See id.*; Tr. 212; Def. Ex. 21 at 8. And Google picked a method of calculating which devices were inside the geofence that generated a high number of false positives—people swept up in the dragnet who were never there at all. *See supra* at 16-17. Google had to do all of this because the warrant did not specify one way or another. The issue is not whether Google should have searched other databases, or taken the Display Radius into account in its search, or whether these decisions were "correct." *See* ECF No. 109 at 18. The issue is that Google is making these decisions instead of a judge. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004). And here, these decisions had measurable consequences: At least one and as many as five of the 19 users identified in step one were likely never within the geofence, with one device that could have been more than 200 meters outside of it. *See* Tr. 42, 64, 587; ECF No. 104 at 8.

Far more troubling is the amount of discretion that the warrant envisioned for the government at steps two and three. At each step, it was up to the government to "narrow" the list of devices and determine which users will be subject to further scrutiny. Def. Ex. 1 at 4–5. Thus, in step two, the government was to decide, in some unspecified manner, which devices they would receive "contextual" data for, *i.e.*, two hours of Location History data without geographic limitation. *Id.* at 4. And in step three, the warrant left it up to the government to pick the accounts for which Google would provide full subscriber information. *Id.* at 5. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See* Fuentes Opinion,

481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); Weisman Opinion, 2020 WL 5491763, at *6 ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way").

Even this process, however, involved additional uncertainty and negotiation over what data the government could seize. After step one, the government repeatedly emailed and called Google to demand step-two "contextual" data, as well as step-three subscriber information on all 19 devices identified in step one. *See supra* at 18-19. It was only because Google refused that the government was unsuccessful, acquiesced, and eventually requested additional data on only nine users. *Id*. The problem is that the Fourth Amendment requires courts, not detectives or companies, to decide what the government can search and seize. Here, the warrant allowed Google and Det. Hylton to decide which accounts to search and "de-anonymize," and Det. Hylton demonstrated why the Fourth Amendment does not trust law enforcement to make that decision.

Step three similarly imbued the government with the sole discretion to decide which people would have their full subscriber information disclosed by Google. The warrant did not identify any of them, or provide any objective criteria by which to identify them. *See* Weisman Opinion, 2020 WL 5491763 at *6 ("For example, the warrant does not limit agents to only seeking identifying information as to the 'five phones located closest to the center point of the geofence,' or some similar objective measure of particularity."). Once again, the decision belonged to the government, not a court. And once again, the government used this discretion to seek additional information about one person who was likely never inside the geofence at all, something that should have been apparent from the step-two data. *See* Tr. 65–66; ECF No. 104 at 27.

At each step, the warrant allowed Google and the government to be the arbiters of what was reasonable to search and seize. No objective observer could look at the warrant and ascertain which accounts the government had authority to "de-anonymize" or obtain "contextual" about. The warrant therefore lacked particularity and violated the Fourth Amendment.

III. The Good Faith Exception Does Not Apply

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is based on "objectively reasonable law enforcement activity." But, *Leon* "good faith" offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted merely as a rubber stamp for the police, *id.* (citing *Illinois v. Gates*, 462 U.S. 213 (1983)); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid, *id.* at 923.

The Supreme Court did not intend for the good faith exception to diminish the power and force of the Fourth Amendment. *Id.* at 924. Rather, the Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923. As Mr. Chatrie has argued, *see* ECF Nos. 48 at 17-20 and 104 at 28-30, the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. As set forth above and in the earlier briefing, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so

obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the magistrate issuing the geofence warrant "abandoned his judicial role" and acted as a rubber stamp here. On June 14, 2019, the police presented the geofence warrant to a magistrate who had served for less than a year, had finished his probationary period a handful of months before, and had only a bachelor's degree from an unlicensed school. *See* ECF Nos. 135-2 at 22 and 156. There is no evidence in this case that the magistrate had any training on geofence warrants or had even seen a geofence warrant before June 14, 2019. On that date, Det. Hylton walked into the magistrate's office where other magistrates were present. Tr. 638. He handed the warrant application to Magistrate Bishop. *Id.* The magistrate looked over the application privately for maybe fifteen or thirty minutes and signed the warrant without asking a single question or making a single change to the warrant. *Id.* at 638-39. While perhaps that type of review may suffice for a more ordinary warrant, a warrant that necessarily requires governmental invasion into the intimate details of many innocent persons' private lives should generate more distress.

The magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as the neutral arbiter between individual privacy and government overreach. The magistrate apparently had no qualms with signing a warrant that—contrary to the Fourth Amendment's patent particularity requirement—allowed the police to search a haystack composed of numerous tens of millions of people's intimate, private data to see if a needle might turn up. The magistrate was further unconcerned that the warrant granted immense discretion to the executing officers and Google to decide what Google data to search. The affidavit in this case did not describe objectively reasonable law enforcement activity. Rather,

it described a general warrant that the framers created the Fourth Amendment to preclude. The particularity requirement "makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 512 (1965); *see also United States v. Wilhelm*, 80 F.3d 116, 121-23 (4th Cir. 1996) (finding that magistrate acted as rubber stamp by abandoning scrutiny of basic tenet of Fourth Amendment); *United States v. Decker*, 956 F.2d 773, 777-78 (8th Cir. 1992) (finding judge did not fulfill role of neutral and detached reviewer by approving warrant with glaring omissions); *United States v. Winn*, 79 F. Supp. 3d 904, 924 (S. D. Ill. 2015) (finding judge acted as rubber stamp "when he signed off on a warrant despite the facially overbroad nature of the list of items to be seized").

Second, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search for Mr. Chatrie's location data that it was entirely unreasonable for any objective officer—i.e., one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements—to rely on. *See Leon*, 468 U.S. at 923. Here, police knew a robbery suspect was carrying what appeared to be a cell phone. Tr. 608. They had no idea what company made the cell phone, what carrier provided service for the phone, what operating system the phone used, or what applications and permissions were installed and actively gathering data on the phone. Rather than trying to do some detective work like track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower, Tr. 578-79, the police decided to get permission to rummage through numerous tens of millions of people's location data simply because the robbery suspect had what appeared to be a cell phone in his hand.

Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (2011) (rejecting good-faith exception where warrant application contained "remarkably scant evidence . . . to support a belief that [the defendant] *in fact* possessed child pornography"); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect's house to the crime under investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013) ("A reasonable police officer would be unable to infer through normal inferences that electronic devices owned by child abusers in general or the Defendant specifically contain evidence related to the criminal activity being investigated . . . ."). That did not happen here. Rather, what happened here was the police obtained a warrant based on conjecture that Google had location data for the cell phone the robbery suspect appeared to be carrying. Obtaining warrants based on conjecture is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Third, the good faith exception should not apply because the geofence warrant was "facially deficient" and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As an initial matter and as set forth above, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases from the First, Eighth, and Ninth Circuits).

Additionally, the extraordinary discretion this warrant purported to authorize renders the warrant facially deficient. Law enforcement agencies and Google worked hand-in-hand in to develop the three-step process outlined above for requesting and responding to geofence warrants. Tr. 455-57, 476. Google, sometimes with police help, gets to decide how big of a geographical area is too big. Tr. 455-58, 461. Google, sometimes with police help, gets to decide if a range of time is too long. Tr. 458-59, 462-64. Google also gets to decide if it does not want to comply with a geofence warrant because it is too sensitive, say for political reasons. Tr. 459-60. Google gets to decide any time limits it wants to apply in between the various steps in the three-step process. Tr. 464-66, 469-70. Google gets to decide if the police have attempted to narrow the information to be seized between the various stages. Tr. 467-69, 471-72. In sum, the three-step process that law enforcement agencies and Google created for Google to respond to geofence warrants entrusts essentially unfettered discretion with the police and Google to execute the warrant.

While Det. Hylton had no training in understanding or applying for geofence warrants, Tr. 627-28, no objective officer could have reasonably believed that a warrant that gave Google and the police unprecedented discretion in executing the warrant was valid. *See George*, 975 F.2d at 76 ("Absent some limitation curtailing the officers' discretion when executing the warrant, the safeguard of having a magistrate determine the scope of the search is lost."); *Leary*, 846 F.2d at 609 ("A warrant that directs an officer to seize records 'relating to' violations of the federal export laws offers no such guidelines. The officers were left to their own discretion."); *see also Winn*, 79 F. Supp. 3d at 924 ("it was not objectively reasonable for the[police] to think that a warrant was valid when it gave them unbridled discretion to search for and seize whatever they wished"). Obtaining warrants authorizing nearly unfettered discretion is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

For any of these reasons, the Court cannot find that the good-faith exception applies to evidence that the government obtained from the geofence warrant and the fruits flowing therefrom. While Mr. Chatrie has not and is not raising a *Franks* claim, the misleading information in the warrant application and material information the police omitted from the warrant certainly reinforces the conclusion that the Court should not apply the good-faith exception in this case. *See Leary*, 846 F.2d at 609-10 (finding that conduct and circumstances of the search reinforced conclusion that "suppression of the evidence is appropriate to deter government misconduct"). In this case, the government falsely told the magistrate that the Google data in the first two stages was anonymous. We know now that a person can reasonably be identified through a handful of location points. Tr. 62-70; ECF 104 at 12; 1/21/20 Tr. at 83, 87-88, 90-91. The Device ID Google uses to identify a device and account remains the same from warrant to warrant. Tr. 451-54. The police did not inform the magistrate that Google would have to search numerous tens of millions of people's private location diaries in stage one. The police also did not inform the magistrate that the geofence would almost certainly capture devices outside of the geofence or that the approximate device locations were only 68% accurate. This level of misinformation and omitted information only underscores that the geofence warrant in this case was not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

CONCLUSION

If ever there were a case to find that the government used a general warrant, then this is it: a dragnet of "numerous tens of millions" paired with unchecked discretion. The warrant was so profoundly overbroad and lacking in particularity that the good faith doctrine should not apply. Mr. Chatrie therefore asks this Court to suppress all evidence obtained from geofence warrant and all of its poisonous fruits.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

_____/s/_____.
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org